REMARKS

In the Official Action mailed **17 April 2006**, the Examiner reviewed claims 49-66. Claims 62-66 were objected to under 37 CFR §1.75(c) as being of improper dependent form for failing to limit the subject matter of a previous claim. Claims 49-60 were rejected under 35 U.S.C. §101 because the claimed invention is directed to non-statutory subject matter. Claims 49-50, 54-56, 60-62, and 66 were rejected under 35 U.S.C. §103(a) as being unpatentable over D. Richard Kuhn (USPN 6,023,765, hereinafter "Kuhn") in view of Sweet et al (USPub 2002/0031230, hereinafter "Sweet"). Claims 51-53, 57-59, and 63-66 were rejected under 35 U.S.C. §103(a) as being unpatentable over Kuhn, in view of Sweet, and further in view of Minear et al. (USPN 5,983,350 hereinafter "Minear").

Objections under 37 CFR §1.75(c)

Claims 62-66 were objected to under 37 CFR §1.75(c) as being of improper dependent form for failing to limit the subject matter of a previous claim.

Applicant has amended claims 62-66 to place the claims in proper dependent form.

Rejections under 35 U.S.C. §101

Independent claims 49, 55, and 61 were rejected under 35 U.S.C. §101 because the claimed invention is directed to non-statutory subject matter.

Applicant has amended independent claims 49, 55, and 61 to clarify that: (1) if the user is a sensitive user, and if the command is received from a normal database administrator, **preventing** the normal database administrator from performing the administrative function involving the sensitive user; and (2) if the user is a sensitive user, and if the command is received from a security officer who is the only database administrator empowered to perform administrative functions involving sensitive users, **performing** the administrative function.

if the user is a sensitive user, and if the command is received from a normal database administrator, the present invention *prevents the normal database administrator from performing the administrative function on the sensitive user.*

Rejections under 35 U.S.C. §103(a)

Independent claims 49, 55, and 61 were rejected as being unpatentable over Kuhn in view of Sweet. Applicant respectfully points out that Kuhn teaches using role-based access control to enhance multi-level secure systems (see Kuhn column 4, lines 25-31). When a user requests a privilege, the role-based access control system determines if the user is allowed to perform the privilege (see Kuhn column 3, lines 64-66; column 7, line 65 to column 8, line 4). Kuhn does not teach a special administrator who manages only sensitive users. In fact, Kuhn teaches **a single administrator** who manages all aspects of the role-based access control system (see Kuhn column 10, lines 5-10).

Sweet teaches a security officer who sets up domain authorities (see Sweet paragraph [0090]). Note that domain authorities provide top-level management to a CKM domain and a subset of administrative tasks (see Sweet paragraphs [0090]-[0102]). One such task is to setup workgroups and workgroup administrators (see Sweet paragraph [0098]). Note that workgroup administrators manage workgroups (see Sweet paragraph [0106]). In other words, Sweet teaches a hierarchy of administrators. Workgroup administrators can add members to workgroups and manage a member's security profile (see Sweet paragraph [0155]), however, the *security officer and the domain authority can also manage* security profiles (see Sweet paragraph [0247]). Under Sweet, even if a special workgroup is created to manage sensitive users, **multiple administrators can manage these sensitive users** (i.e., security officer, domain authority, workgroup administrator).

In contrast, the present invention manages a database system that provides the capability to store sensitive data in encrypted form, while minimizing the number of database administrators who can access the encrypted data (see page 2,

line 26 to page 3, line 2 of the instant application). Allowing multiple database administrators to access sensitive data increases the chance that a *rogue database administrator* can obtain the sensitive data. The present invention teaches a special administrator, **the security officer**, who is the **only administrator** allowed to perform administrative functions on sensitive users and sensitive objects (see page 7, lines 7-11; page 8, lines 19-20; and page 9, line 4 to page 10, line 3 of the instant application). Hence, in the present invention, it is not possible for normal system administrators to gain access to sensitive data.

There is nothing in Kuhn or Sweet, either separately or in concert, which suggests protecting sensitive data and sensitive users using a *security officer who is the only database administrator empowered to perform administrative functions on sensitive users.*

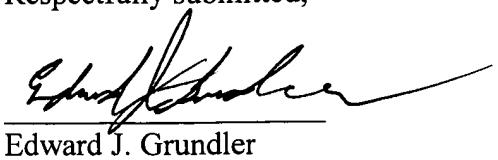
Accordingly, Applicant has amended independent claims 49, 55, and 61, to clarify that the present invention uses a *security officer who is the only database administrator empowered to perform administrative functions on sensitive users.* These amendments find support on page 7, lines 7-11; page 8, lines 19-20; and page 9, line 4 to page 10, line 3 of the instant application.

Hence, Applicant respectfully submits that independent claims 49, 55, and 61 as presently amended are in condition for allowance. Applicant also submits that claims 50-54, which depend upon claim 49, claims 56-60, which depend upon claim 55, and claims 62-66, which depend upon claim 61 are for the same reasons in condition for allowance and for reasons of the unique combinations recited in such claims.

CONCLUSION

It is submitted that the present application is presently in form for allowance. Such action is respectfully requested.

Respectfully submitted,

By 

Edward J. Grundler
Registration No. 47,615

Date: 9 May 2006

Edward J. Grundler
PARK, VAUGHAN & FLEMING LLP
2820 Fifth Street
Davis, CA 95616-7759
Tel: (530) 759-1663
FAX: (530) 759-1665
Email: edward@parklegal.com